(2)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-101566
(43)Date of publication of application : 04.04.2003

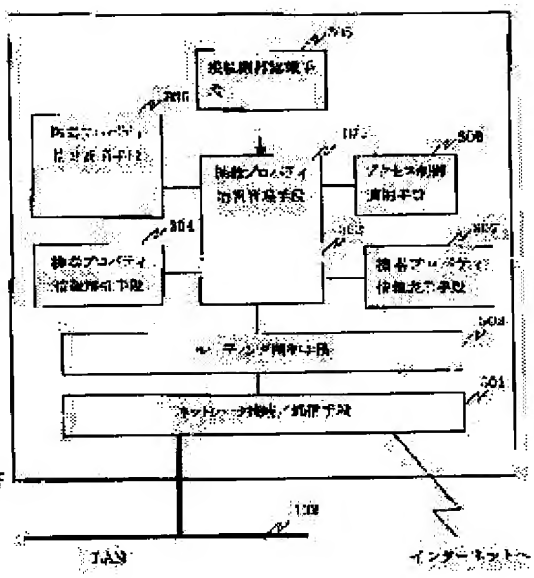
(51)Int.Cl. H04L 12/46
G06F 13/00

(21)Application number : 2001-285808
(22)Date of filing : 19.09.2001

(71)Applicant : HITACHI SOFTWARE ENG CO LTD
(72)Inventor : KOYAKATA TAKEHIRO

(54) NETWORK EQUIPMENT MANAGEMENT METHOD AND SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To assure a certain level of security without impairing the convenience of Plug and Play and enable management of equipment connected to a network without requiring expertise or burdensome work.
SOLUTION: The system comprises: a connected equipment recognizing means for automatically recognizing equipment connected to a LAN, an equipment property information storing means for storing equipment property information including identifiers to uniquely identify the equipment connected to the LAN and additional information about each of the equipment, a display means for displaying the equipment property information, and a management means for managing the equipment connected to the LAN based on the equipment property information stored in the equipment property information storing means. The method comprises the steps of: determining whether the equipment recognized by the connected equipment recognizing means is registered equipment or not by referring to the property information stored in the property information storing means, and, in the case of unregistered equipment, displaying notification to that effect on the screen of a display device.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－101566
（P2003－101566A）
(43)公開日　平成15年４月４日(2003.4.4)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　12/46	Ｍ　５Ｂ０８９
Ｇ０６Ｆ　13/00	３５７	Ｇ０６Ｆ　13/00	３５７Ａ　５Ｋ０３３

審査請求　未請求　請求項の数14　ＯＬ　（全 14 頁）

(21)出願番号　特願2001－285808(P2001－285808)

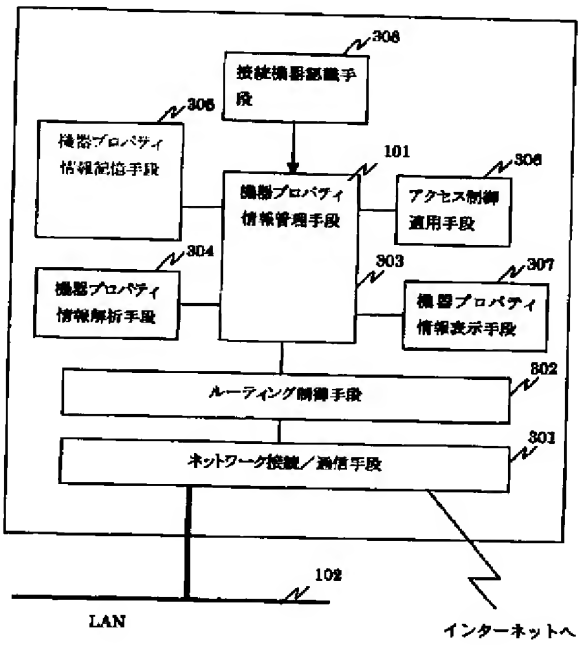
(22)出願日　平成13年９月19日(2001.9.19)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市鶴見区末広町一丁目１番43
(72)発明者　古舘　丈裕
神奈川県横浜市中区尾上町６丁目81番地　日立ソフトウエアエンジニアリング株式会社内
(74)代理人　100088720
弁理士　小川　眞一

Ｆターム(参考)　5B089 GB02 HA06 JA35 JB15 KA13 KB03 KB06 KC59
5K033 AA08 AA09 DB20 EC02 EC03

(54)【発明の名称】　ネットワーク機器の管理方法および装置

(57)【要約】
【課題】　プラグアンドプレイの利便性を損なうことなく一定のセキュリティレベルを確保し、高度な知識と負荷の高い作業を必要とせずにネットワーク上に接続される機器を管理することを可能にする。
【解決手段】　ＬＡＮに接続された機器を自動的に認識する接続機器認識手段と、ＬＡＮに接続された機器を一意に識別する識別子とそれぞれの機器に関する付加情報を含む機器プロパティ情報を記憶した機器プロパティ情報記憶手段と、機器プロパティ情報を表示する表示手段と、前記機器プロパティ情報記憶手段に記憶された機器プロパティ情報に基づいてＬＡＮに接続された機器を管理する管理手段とを備え、前記接続機器認識手段によって認識した機器が既に登録されている機器であるかを前記プロパティ情報記憶手段に記憶されたプロパティ情報を参照して判定するステップと、未登録の機器であれば、その旨を表示装置画面に表示するステップとを備えることを特徴とする。



1

【特許請求の範囲】

【請求項１】　ＬＡＮに接続された機器を自動的に認識する接続機器認識手段と、ＬＡＮに接続された機器を一意に識別する識別子とそれぞれの機器に関する付加情報を含む機器プロパティ情報を記憶した機器プロパティ情報記憶手段と、機器プロパティ情報を表示する表示手段と、前記機器プロパティ情報記憶手段に記憶された機器プロパティ情報に基づいてＬＡＮに接続された機器を管理する管理手段とを備えるネットワーク機器管理装置におけるネットワーク機器の管理方法であって、

前記接続機器認識手段によって認識した機器が既に登録されている機器であるかを前記プロパティ情報記憶手段に記憶されたプロパティ情報を参照して判定するステップと、

未登録の機器であれば、その旨を表示装置画面に表示するステップとを備えることを特徴とするネットワーク機器の管理方法。

【請求項２】　前記未登録の機器に対する登録指示と該機器のプロパティ情報を受付け、前記機器プロパティ情報記憶手段に記憶させるステップとをさらに備えることを特徴とする請求項１に記載のネットワーク機器の管理方法。

【請求項３】　前記未登録の機器に対する機器プロパティ情報を、当該機器固有の識別子と機器のプロパティ情報とを関連付けたデータベースからインターネットを介して取得し、前記機器プロパティ情報記憶手段に記憶させるステップとをさらに備えることを特徴とする請求項１に記載のネットワーク機器の管理方法。

【請求項４】　機器プロパティ情報のスキーマ定義を、機器プロパティ情報のスキーマ定義情報を持つデータベースからインターネットを通して取得し、前記機器プロパティ情報のスキーマを動的に変更し、対応する機器プロパティ情報のインスタンスを新しいスキーマに合致するように自動的に修正するステップをさらに備えることを特徴とする請求項１～３のいずれか一項に記載のネットワーク機器の管理方法。

【請求項５】　ＬＡＮ上の機器から受信したパケットのインターネットへのフォワード、あるいはインターネットから受信したパケットのＬＡＮ上の機器へのフォワードに対して、送信元もしくは宛先となる機器が登録済みの機器であるかどうかによって、フォワードを許可するかどうかの設定指示を受付け、その設定指示に応じて、前記機器プロパティ情報記憶手段に記憶させるステップをさらに備えることを特徴とする請求項１～４のいずれか一項に記載のネットワーク機器の管理方法。

【請求項６】　ＬＡＮに接続されている機器同士での通信を許可するかどうかの登録指示を、登録済み機器か未登録機器かの組み合わせに応じて受付け、指示内容に従って前記機器プロパティ情報記憶手段に記憶させるステップをさらに備えることを特徴とする請求項１～５のいずれか一項に記載のネットワーク機器の管理方法。

2

【請求項７】　同一種別の機器について同一の機器プロパティ情報を設定するステップを備えることを特徴とする請求項５または６記載のネットワーク機器の管理方法。

【請求項８】　ＬＡＮに接続された機器を自動的に認識する接続機器認識手段と、ＬＡＮに接続された機器を一意に識別する識別子とそれぞれの機器に関する付加情報を含む機器プロパティ情報を記憶した機器プロパティ情報記憶手段と、機器プロパティ情報を表示する表示手段と、前記機器プロパティ情報記憶手段に記憶された機器プロパティ情報に基づいてＬＡＮに接続された機器を管理する管理手段とを備えるネットワーク機器管理装置であって、

前記接続機器認識手段によって認識した機器が既に登録されている機器であるかを前記プロパティ情報記憶手段に記憶されたプロパティ情報を参照して判定する手段と、

未登録の機器であれば、その旨を表示装置画面に表示する手段とを備えることを特徴とするネットワーク機器の管理装置。

【請求項９】　前記未登録の機器に対する登録指示と該機器のプロパティ情報を受付け、前記機器プロパティ情報記憶手段に記憶させる手段とをさらに備えることを特徴とする請求項８に記載のネットワーク機器の管理装置。

【請求項１０】　前記未登録の機器に対する機器プロパティ情報を、当該機器固有の識別子と機器のプロパティ情報とを関連付けたデータベースからインターネットを介して取得し、前記機器プロパティ情報記憶手段に記憶させる手段とをさらに備えることを特徴とする請求項８に記載のネットワーク機器の管理装置。

【請求項１１】　機器プロパティ情報のスキーマ定義を、機器プロパティ情報のスキーマ定義情報を持つデータベースからインターネットを通して取得し、前記機器プロパティ情報のスキーマを動的に変更し、対応する機器プロパティ情報のインスタンスを新しいスキーマに合致するように自動的に修正する手段をさらに備えることを特徴とする請求項８～１０のいずれか一項に記載のネットワーク機器の管理装置。

【請求項１２】　ＬＡＮ上の機器から受信したパケットのインターネットへのフォワード、あるいはインターネットから受信したパケットのＬＡＮ上の機器へのフォワードに対して、送信元もしくは宛先となる機器が登録済みの機器であるかどうかによって、フォワードを許可するかどうかの設定指示を受付け、その設定指示に応じて、前記機器プロパティ情報記憶手段に記憶させる手段をさらに備えることを特徴とする請求項８～１１のいずれか一項に記載のネットワーク機器の管理装置。

【請求項１３】　ＬＡＮに接続されている機器同士での

通信を許可するかどうかの登録指示を、登録済み機器か未登録機器かの組み合わせに応じて受付け、指示内容に従って前記機器プロパティ情報記憶手段に記憶させる手段をさらに備えることを特徴とする請求項８～１２のいずれか一項に記載のネットワーク機器の管理装置。

【請求項１４】　同一種別の機器について同一の機器プロパティ情報を設定する手段を備えることを特徴とする請求項１２または１３記載のネットワーク機器の管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンピュータネットワーク上に接続される機器の管理方法および装置に係り、特に家庭向けのＬＡＮ(Local Area Network)環境において、専門的な知識が無くてもＬＡＮに接続されるパーソナルコンピュータ（ＰＣ）や家電などの機器を簡単な操作のみで管理できるようにするネットワーク機器の管理方法および装置に関するものである。

【０００２】

【従来の技術】インターネットプロトコルIPv6が実用段階に入ったこととあいまって、コンピュータネットワークの利用状況が幾つかの点でこれまでとは変わってきている。１つは、ネットワークに接続される機器の多様化である。これまではネットワークに接続される機器といえば、ＰＣやワークステーション、プリンタなどの機器、あるいはルータやスイッチ、ハブなどのネットワーク機器が主なものであった。しかし、今後は、冷蔵庫やテレビ、エアコンといった一般的な家電製品の他、温度／湿度計などのセンサ類、自動車に設置した速度計などもネットワーク化され、ネットワークを通して稼動状況を調べたり、動作を制御しようとしたりする方向に向かいつつある。また、ネットワークが構築される場所も、これまでの大学や企業などから、一般の家庭や商店などに徐々に広まってきている。

【０００３】もう１つは、ネットワークに接続される機器の台数の増加である。ＩＰアドレスの枯渇問題がＩＰｖ６の実用化によって解決される目処がたったことから、これまでに比べて多数の機器がネットワークに接続されることは容易に予想される。それに応じてネットワークの管理にかかる作業量も増加すると考えられる。大量の機器についてＩＰアドレスなどを１つ１つ設定していくのは大変負荷の高い作業になるので、プラグアンドプレイ機能による自動接続が主流となりつつある。

【０００４】プラグアンドプレイ機能には、割り当てるＩＰアドレスを予めプールしておくステートフル方式と、アドレスのプールを必要としないステートレス方式がある。ステートフル方式としては、ＤＨＣＰ(Dynamic Host Configuration Protocol)という仕組みが実現されている。ステートレス方式はＩＰｖ６で規格化されている方式であり、ネットワークのセグメントに対して、ネットワークのプレフィックス情報（ネットワークアドレスなど）を含んだルータ通知を発行し、各ネットワーク機器は通知されたネットワークプレフィックスと自身のインタフェース識別子を利用してＩＰアドレスを自動生成する。このようなプラグアンドプレイ機能を用いることで、管理者の負担を増やさずに、多くの機器を簡単にネットワークに接続することができるようになっている。特に、ＩＰｖ６の使用が主流になるようになれば、その手軽さからステートレスなプラグアンドプレイで運用されるネットワークが多くなると予想される。

【０００５】

【発明が解決しようとする課題】しかし、特別な設定をすることなく自動的にネットワークに接続できるということは、ネットワーク管理者が意図していない不正な機器も簡単に接続できてしまうことを意味する。特に、無線ＬＡＮ環境においてプラグアンドプレイを実施している場合は、接続ケーブル等による物理的な接続も不要なため、非常に簡単にネットワークに接続できてしまう。そのため、例えば、ＬＡＮの管理者または利用者が知らない間に不正な機器が接続され、ＬＡＮ上で提供されているサービスを不正に利用されたり、不正に情報を持ち出されたりすることが起こり得る。

【０００６】そこで、管理者が認めた特定の機器だけが接続できるようにするために、接続を許可する機器を一意に識別する何らかの識別子を予め登録しておき、接続時に認証する手順を実施することが考えられる。しかし、全ての機器について登録を行おうとすると、プラグアンドプレイの恩恵が全く受けられなくなり、機器数が多い場合の登録作業量が膨大になってしまう。すなわち、プラグアンドプレイの利便性と不正な機器の接続によるセキュリティ上の脅威とのジレンマに陥ることになる。また、ネットワークの管理作業はコンピュータやネットワークに関する深い知識を必要とする。これまでの大学や企業におけるネットワークでは、相応の技術をもった人員が管理作業を担当していた。しかし、一般の家庭でのネットワークを構築する場合には、必ずしも必要な技術を持った人員を確保できるとは限らない。ゲートウェイ製品によっては、Ｗｅｂブラウザからメニューを選択する形式で簡単に設定が行えるものもあるが、それでもＩＰやその上位プロトコルのＴＣＰやＵＤＰ、あるいはＤＮＳの仕組み等について十分な知識を持っていなければ、どれを選択して良いか判断できない。

【０００７】更に、これまでは、例えばパケットフィルタリングの設定をする際には、個々の機器をＩＰアドレスで一意に指定するか、同じサブネット上の機器をひとまとめにして指定していた。しかし、ネットワークに多数の機器が接続されるような環境では、個別に設定するのでは作業の負荷が非常に高くなってしまう。機器を幾つかのグループに分類して、グループごとに設定できるようになれば、管理作業を軽減することができる。

5

【０００８】本発明の目的は、プラグアンドプレイの利便性を損なうことなく一定のセキュリティレベルを確保し、高度な知識と負荷の高い作業を必要とせずにネットワーク上に接続される機器を管理することができるネットワーク機器の管理方法および装置を提供することにある。

【０００９】

【課題を解決するための手段】上記目的を達成するために、本発明は、ＬＡＮに接続された機器を自動的に認識する接続機器認識手段と、ＬＡＮに接続された機器を一意に識別する識別子とそれぞれの機器に関する付加情報を含む機器プロパティ情報を記憶した機器プロパティ情報記憶手段と、機器プロパティ情報を表示する表示手段と、前記機器プロパティ情報記憶手段に記憶された機器プロパティ情報に基づいてＬＡＮに接続された機器を管理する管理手段とを備えるネットワーク機器管理装置におけるネットワーク機器の管理方法であって、前記接続機器認識手段によって認識した機器が既に登録されている機器であるかを前記プロパティ情報記憶手段に記憶されたプロパティ情報を参照して判定するステップと、未登録の機器であれば、その旨を表示装置画面に表示するステップとを備えることを特徴とする。また、前記未登録の機器に対する登録指示と該機器のプロパティ情報を受付け、前記機器プロパティ情報記憶手段に記憶させるステップとをさらに備えることを特徴とする。また、前記未登録の機器に対する機器プロパティ情報を、当該機器固有の識別子と機器のプロパティ情報とを関連付けたデータベースからインターネットを介して取得し、前記機器プロパティ情報記憶手段に記憶させるステップとをさらに備えることを特徴とする。また、機器プロパティ情報のスキーマ定義を、機器プロパティ情報のスキーマ定義情報を持つデータベースからインターネットを通して取得し、前記機器プロパティ情報のスキーマを動的に変更し、対応する機器プロパティ情報のインスタンスを新しいスキーマに合致するように自動的に修正するステップをさらに備えることを特徴とする。また、ＬＡＮ上の機器から受信したパケットのインターネットへのフォワード、あるいはインターネットから受信したパケットのＬＡＮ上の機器へのフォワードに対して、送信元もしくは宛先となる機器が登録済みの機器であるかどうかによって、フォワードを許可するかどうかの設定指示を受付け、その設定指示に応じて、前記機器プロパティ情報記憶手段に記憶させるステップをさらに備えることを特徴とする。また、ＬＡＮに接続されている機器同士での通信を許可するかどうかの登録指示を、登録済み機器か未登録機器かの組み合わせに応じて受付け、指示内容に従って前記機器プロパティ情報記憶手段に記憶させるステップをさらに備えることを特徴とする。また、同一種別の機器について同一の機器プロパティ情報を設定するステップを備えることを特徴とする。

6

【００１０】本発明に係るネットワーク機器の管理装置は、ＬＡＮに接続された機器を自動的に認識する接続機器認識手段と、ＬＡＮに接続された機器を一意に識別する識別子とそれぞれの機器に関する付加情報を含む機器プロパティ情報を記憶した機器プロパティ情報記憶手段と、機器プロパティ情報を表示する表示手段と、前記機器プロパティ情報記憶手段に記憶された機器プロパティ情報に基づいてＬＡＮに接続された機器を管理する管理手段とを備えるネットワーク機器管理装置であって、前記接続機器認識手段によって認識した機器が既に登録されている機器であるかを前記プロパティ情報記憶手段に記憶されたプロパティ情報を参照して判定する手段と、未登録の機器であれば、その旨を表示装置画面に表示する手段とを備えることを特徴とする。また、前記未登録の機器に対する登録指示と該機器のプロパティ情報を受付け、前記機器プロパティ情報記憶手段に記憶させる手段とをさらに備えることを特徴とする。また、前記未登録の機器に対する機器プロパティ情報を、当該機器固有の識別子と機器のプロパティ情報とを関連付けたデータベースからインターネットを介して取得し、前記機器プロパティ情報記憶手段に記憶させる手段とをさらに備えることを特徴とする。また、機器プロパティ情報のスキーマ定義を、機器プロパティ情報のスキーマ定義情報を持つデータベースからインターネットを通して取得し、前記機器プロパティ情報のスキーマを動的に変更し、対応する機器プロパティ情報のインスタンスを新しいスキーマに合致するように自動的に修正する手段をさらに備えることを特徴とする。また、ＬＡＮ上の機器から受信したパケットのインターネットへのフォワード、あるいはインターネットから受信したパケットのＬＡＮ上の機器へのフォワードに対して、送信元もしくは宛先となる機器が登録済みの機器であるかどうかによって、フォワードを許可するかどうかの設定指示を受付け、その設定指示に応じて、前記機器プロパティ情報記憶手段に記憶させる手段をさらに備えることを特徴とする。また、ＬＡＮに接続されている機器同士での通信を許可するかどうかの登録指示を、登録済み機器か未登録機器かの組み合わせに応じて受付け、指示内容に従って前記機器プロパティ情報記憶手段に記憶させる手段をさらに備えることを特徴とする。また、同一種別の機器について同一の機器プロパティ情報を設定する手段を備えることを特徴とする。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて詳細に説明する。図１は本発明を利用するネットワーク環境の一例を示す図である。図１において、１０１は本発明を適用したルータ兼ネットワーク機器管理装置（以下、ネットワーク管理装置と略記）である。１０２はＬＡＮを模式的に示したものであり、実際には10BaseTなどのケーブルとハブによる実現や、無線ＬＡ

Ｎによる実現が利用できる。ネットワーク管理装置１０１はこのＬＡＮ１０２と接続すると共に、外部のインターネットとも接続するルータの役割を果たす。ＬＡＮ１０２上には、Ｗｅｂサーバなどのサーバの機能を持つ登録済みサーバ機器１０３と、このサーバ機器１０３に対してアクセスするクライアントとなる登録済みクライアント機器１０４および未登録クライアント機器１０５が接続される。

【００１２】本実施形態では、ＬＡＮ１０２に接続する機器の重要度レベルとして、予めその機器を一意に識別する識別子を登録している登録済み機器と、識別子を登録していない未登録機器の２種類を設定している。ここでは、サーバ機器１０３とクライアント機器１０４が登録済み機器であり、もう１つのクライアント機器１０５が未登録機器である。

【００１３】このようなネットワーク構成の下で、本発明においては、登録済み機器と未登録機器に対して、ネットワーク上で利用できるサービスの内容をそれぞれ別々に設定することができる。ここでいうサービスとは、インターネット上へのパケットの送信、インターネットからのパケットの受信、ＬＡＮ上の登録済みの機器へのパケットの送信、登録済みの機器からのパケットの受信、ＬＡＮ上の未登録の機器へのパケットの送信、未登録の機器からのパケットの受信のことを指す。本発明においては、プラグアンドプレイの利便性とセキュリティレベルの保持とのジレンマおよびネットワーク管理作業に高度な知識と負荷の高い作業が要求されることに対して、次のような方法で解決を図っている。

【００１４】まず、ＬＡＮに接続される機器間で重要度のレベルを設定し、重要度レベルの高い機器だけを登録と認証を必須とし、プラグアンドプレイで接続可能とする機器は低いレベルに自動的に調整されるようにする。そして、重要度レベルの異なる機器間、あるいは同一レベルの機器間での通信を設定できるようにする。このようにすることで、高いレベルを設定した機器に関しては登録作業が必要になってしまうが、それだけの安全性を確保しつつ、かつ、重要度のレベルを低く設定した機器ではプラグアンドプレイの利便性を活かすことができる。センサ類のように主な目的がデータの送出で不正な機器からアクセスされてもあまり深刻な問題が発生せず、かつ、数が多くなり易い機器はプラグアンドプレイを利用可能にし、サーバ用ＰＣのような不正アクセスによって被害が大きくなり易いものは登録制にするという運用とすることによって、従来技術の問題を改善できることが期待できる。なお、プラグアンドプレイ機能は図１のネットワーク機器管理装置１０１内に設けられるものであるが、図３においては接続機器認識手段３０８で示している。また、認識した機器の重要度が高いかどうかは、管理者が判定するしかないので、自動認識した機器が登録されていない機器であれば、その旨を表示し、管理者に重要度を判定させ、その判定結果に従って、登録手続を行う、または行わないような仕組みを用意している。

【００１５】ネットワーク管理作業の簡略化については、機器をグループ化して同じグループの機器に関しては設定をひとまとめにすることで解決を図る。グループの分け方としては、「冷蔵庫」や「温度計」といった機器の種別のような、抽象的な分類ができれば理解し易くなる。しかし、この分類を全ての機器について手作業で行っていたのでは作業の簡略化にはならない。機器のＭＡＣアドレスのような識別子から、自動的に機器が分類できるような仕組みが望ましい。そのために、ＭＡＣアドレス値からその機器に関する情報を取得できるデータベースを構築し、インターネットを通して参照できるようにすれば良い。ちょうど、ＩＰアドレスからホスト名を逆引きするＤＮＳと同様の分散データベースである。

【００１６】しかし、ホスト名の場合とは異なり、機器情報は構造を持ったデータ構造であり、しかも新しい種類の機器が出現するたびに機器情報のスキーマの変更が起こり得る。そのため、ＤＮＳとは異なり、機器情報データベースではスキーマの変更も伝播させ、それに応じて既存のインスタンスの構造も修正する機能が必要になる。そのために機器情報の構造をＸＭＬで記述することで、スキーマを柔軟に拡張できるようにする。

【００１７】図２は、登録済み機器か未登録機器かによって前記のサービスのどれを利用できるかの典型的な設定例を示す図である。図２において、符号２０１で示す列は登録済み機器のデフォルト設定例であり、この場合は未登録機器へのパケット送信だけを禁止、他の全てのサービスを利用できるように設定している。また、符号２０２で示す列は、未登録機器でのデフォルト設定例であり、インターネットへのパケット送受信とＬＡＮ上の登録済み機器からのパケットの受信を禁止し、登録済み機器へのパケットの送信と、未登録機器同士でのパケット送受信は利用可能に設定している。この設定は、ネットワーク１０２に接続される全ての機器について実施される。未登録済み機器がこの設定通りに登録済み機器からパケットを受信することを禁止する手順を示す前に、最初に、ネットワーク機器管理装置の内部構成について図３のブロック図を参照して説明する。

【００１８】図３は本実施形態におけるネットワーク機器管理装置１０１の内部構成を示すブロック図である。図３において、３０１は本装置がＬＡＮやインターネットと接続するためのネットワーク接続／通信手段であり、通常のネットワーク機器と同等のものである。３０２はＩＰｖ６パケットのルーティングと接続されているネットワークセグメントに対してルータ通知を行う部分であり、通常のＩＰｖ６対応ルータと同様の働きをする。３０３は本実施形態の中心的な役割を担う部分であり、機器プロパティ情報の内容に応じて他の部分に指示

を出したり、機器プロパティ情報のアップデートを行ったりする機器プロパティ情報管理手段である。３０４は機器プロパティ情報を読み込んでエラーチェックすると共に内容を解釈する機器プロパティ情報解析手段である。３０５は登録済みの機器のプロパティ情報を保持するデータベースおよび検索機能を提供する機器プロパティ情報記憶手段である。３０６は機器プロパティ情報の内容と受信したパケットの内容に基づいて、受信したパケットをどのように処理するか判定するアクセス制御適用手段である。３０７はＬＡＮ１０２に接続されている機器の一覧を表示する機器プロパティ情報表示手段である。

【００１９】以上の構成例の上で、以下の事項を実施する手段を順に説明する。

（１）登録済み機器と未登録機器の一覧を、ＬＡＮに接続されているかどうかを含めて表示する。

（２）未登録の機器のプロパティ情報を正当な機器として登録する。

（３）識別子ＤＢから機器の種別を問い合わせる。

（４）スキーマ情報のダウンロードと機器プロパティ情報インスタンスのアップデートを行う。

（５）登録の有無に基づく、インターネットとのルーティング制御手順。

（６）登録の有無に基づく、ＬＡＮ上の他の機器とのアクセス制御の手順。

（７）機器の種別によるアクセス制御手順。

【００２０】図４は、機器プロパティ情報とそのスキーマ情報の記述例である。この例では、拡張性を保持するためにＸＭＬ(Extensible Markup Language)で記述している。４０１は、図１のネットワーク機器管理装置１０１が保持する機器プロパティ情報の内容を記述したＸＭＬインスタンスである。このインスタンス４０１には、２つの機器の情報が記述されている。４０２は１つの機器のプロパティ情報を記述している部分であり、この例ではこの機器がビデオデッキであることを記述している。４０３はもう１つの機器のプロパティ情報であり、この例ではこの機器がパソコンであることを示している。４０４はこれらのインスタンスの記述方法を定義しているＤＴＤ(Document Type Definition；文書型定義)である。

【００２１】この例では、機器プロパティ情報は、devicelist中にdeviceとして列挙され、deviceの内容は２行目のinterface、v4addr、role、maker、optionから構成されることを示している。ここでは、interfaceは機器を一意に特定する識別子を意味しており、この例ではＭＡＣアドレスが記述されている。v4addrはこの機器に割り振られているIPv4アドレス値を、roleはこの機器の種別を、makerはこの機器を製作したメーカ、optionはユーザが付加するその他の情報を意味しており、optionには属性値を付けられるようになっている。すなわち、プロパティ情報４０３のように、置き場所を意図するlocationや持ち主を意図するownerなどの属性を付加できるようになっている。

【００２２】図５は、ネットワーク機器管理装置１０１の外観の一例を示す図である。この装置１０１は筐体５０１と画面５０２、各種の操作ボタン５０５から成る。画面５０２には、機器の一覧が表示される。画面の内容は、図３で示した機器プロパティ情報表示手段３０７によって表示される。この画面例では、ゲートウェイ、パソコンなどの５つの機器のそれぞれについて、識別子、機器種別、登録の状況、接続の状況（稼動中、停止）を表示している。５０３は現在選択されている機器を表している。また、符号５０４のように、未登録の機器が接続されている場合は反転表示などで強調される。

【００２３】図６は、図５で示したような画面を表示する手順を示したフローチャートである。まず、ネットワーク機器管理装置はICMP echo requestを同一セグメント上にマルチキャスト(ブロードキャスト)して、稼動中の機器からecho replyを受信する(ステップ６０１)。そして、受信したパケットの内容からＭＡＣアドレスを取り出し、稼動中機器のＭＡＣアドレスのリストを作成する(ステップ６０２)。次に、図３の機器プロパティ情報ＤＢ３０５に登録済みの機器プロパティ情報があるかどうかを問い合わせ（ステップ６０３）、ある場合は機器プロパティ情報を１件取り出して稼動中機器リストとＭＡＣアドレスを照合する（ステップ６０４）。もし、機器プロパティ情報のinterfaceに示されているＭＡＣアドレスと同じ値が稼動中機器リスト中に存在するならば（ステップ６０５）、その機器が稼動中であると判定し、機器情報を画面に表示する（ステップ６０６）。そして、表示した機器については稼動中機器リストから削除する（ステップ６０７）。

【００２４】ステップ６０５で、もしＭＡＣアドレスが一致するものが稼動中機器リストに無かったならば、その機器が停止中であると判定し、その機器情報を画面に表示する（ステップ６０８）。そして、ステップ６０５から６０８までは、機器プロパティ情報ＤＢ３０５から全ての機器プロパティ情報を取り出すまで繰り返す。全ての登録済み機器の情報を表示した後に、稼動中機器リストに項目が残っているかを調べ（ステップ６０９）、もし残っていた場合は、それらは未登録の機器であると判定して、未登録機器として画面に表示する（ステップ６１０）。未登録機器を正当な機器として登録する場合は、機器がＬＡＮ１０２に接続され未登録機器として画面に表示されている状態で、管理者は登録したい機器を選択し、登録を指示することから始める。

【００２５】図７に以降の手順のフローチャートを示す。まず、ネットワーク機器管理装置１０１は、パスワード入力画面を表示し、管理者に対してパスワードの入力を要求し、入力されたパスワードを照合する（ステッ

プ７０１）。認証が成功した場合は、対象機器のプロパティ情報の入力画面を表示する（ステップ７０２）。入力画面で入力を促す項目は、図４のスキーマ情報４０４の示されているELEMENTの項目に従って作成する。この時、interfaceの項目は、接続時に取得したＭＡＣアドレスの値を予め表示しておく。

【００２６】管理者が各項目を入力し確定すると、ネットワーク機器管理装置１０１は、入力された情報から図４の例のような機器プロパティ情報のＸＭＬインスタンスを生成する（ステップ７０３）。次に、必要な項目が入力されているかチェックし、エラーが無ければ、生成したＸＭＬインスタンスを機器プロパティ情報ＤＢ３０５に格納する（ステップ７０４）。最後に、画面に未登録機器として表示されていた内容を更新する（ステップ７０５）。

【００２７】ところで、ＭＡＣアドレスから機器の種別を調べるためには、ＭＡＣアドレス値から対応する機器のプロパティ情報を検索する共通のデータベースが必要になる。これは、原理的にはＤＮＳ(domain Name System)と同様の分散データベースシステムである。この分散ＤＢは、図８（ａ），（ｂ）に示すような２つのテーブル８０１，８０２を保持する。テーブル８０１はＭＡＣアドレスの前半のメーカ識別子をキーとして、問合せ先ＩＰアドレス値を持つテーブルである。また、テーブル８０２は製品識別子をキーとして、機器プロパティ情報の格納先を持つテーブルである。

【００２８】図９に、分散ＤＢにおける機器種別の問合せ処理手順のフローチャートを示す。分散ＤＢは、ＭＡＣアドレスを引数として問合せを受け付けると、まず後半の製品識別子を元に図８（ｂ）のテーブル８０２を検索し（ステップ９０１）、一致する識別子を持つレコードがあるかどうか調べる（ステップ９０２）。製品識別子の一致するレコードがあった場合は、格納先に示されたＸＭＬインスタンスに含まれる機器種別の情報を返す（ステップ９０３）。無かった場合は、ＭＡＣアドレスの前半のメーカ識別子を元に図８（ａ）のテーブル８０１を検索する（ステップ９０４）。レコードが見つかった場合は（ステップ９０５）、そのレコードに記されているＩＰアドレスで示されるサーバに対して問合せを転送し、得られた結果を最初の問合せ元に返す（ステップ９０６）。レコードが見つからなかった場合は、機器種別が定義されていない旨を問合せの結果として返す（ステップ９０７）。これにより、製品識別子またはメーカ識別子によって機器プロパティ情報を得ることができる。

【００２９】次に、分散ＤＢで管理されている機器プロパティ情報のスキーマが変更された場合に、それをネットワーク機器管理装置１０１が保持する機器プロパティ情報ＤＢに反映させる手順について説明する。ネットワーク機器管理装置１０１は、現在のスキーマのバージョン番号と問合せ先分散ＤＢのアドレスリストを機器プロパティ情報ＤＢ３０５内に保持しておき、リストに示された分散ＤＢに対して定期的にバージョン確認問合せを発行する。バージョン確認問合せの引数には、ネットワーク機器管理装置１０１が保持するスキーマのバージョン番号が含まれる。バージョン確認問合せを受け取った分散ＤＢは、問合せの引数のバージョン番号が、自身が保持するバージョン番号と同じ場合は何もしないが、自身が保持するバージョン番号の方が大きい値の場合は、スキーマ情報、すなわち機器プロパティ情報のＤＴＤと、必要なら追加エレメントのデフォルト値を返す。

【００３０】ネットワーク機器管理装置１０１は、もし新しいバージョンのＤＴＤが返ってきた場合には、古いＤＴＤを問い合わせ結果に含まれている新しいＤＴＤに入れ替える。この時、ＤＴＤの変更内容によっては、機器プロパティ情報のＸＭＬインスタンスを全て更新する必要がある場合がある。例えば、古いＤＴＤでは定義されていたエレメントが新しいＤＴＤでは削除されていたり位置が変わっていたりする場合には、新しいＤＴＤにマッチするようにインスタンスの構造を変更する。あるいは、新しいエレメントが追加されており、そのエレメントが必ず１回以上出現しなければならないように指定されている場合は、全てのインスタンスに、問い合わせ結果に含まれているデフォルト値を持つエレメントを挿入する。エレメントが追加されている場合でも、必ずしも出現しなくても良い場合、すなわち、ＤＴＤ内でクエスチョンマークや“＊”が指定されている場合は出現数が０でも良いのでインスタンスに修正を加える必要はない。これらの処理は機器プロパティ情報を示すＸＭＬインスタンスに対してテキスト処理を施すことで実現できる。このような手順を踏むことにより、ネットワーク機器管理装置１０１は、機器プロパティ情報を常に最新の状態に保つことができる。

【００３１】次に、ＬＡＮ１０２に接続されている機器が登録済み機器か未登録機器かによって、他の機器との通信やインターネットとの接続を制限する手順について説明する。まずは、ＬＡＮ１０２上で行える通信を、その内容によって幾つかのサービスとして定義する。図１０は、サービス定義の一例である。図１０において、１００１はサービスの一覧を記述したＸＭＬインスタンスである。この例では、ForwardToInternet、ForwardFromInternet、SendToRegNode、ReceiveFromRegNode、SendToUnknownNode、ReceiveFromUnknownNodeの６種類のサービスが設定されている。これらは図２に示したサービスをそれぞれ表したものであり、それぞれ「ルータを通してのパケットをインターネットへ送信」、「インターネット側から送られてきたパケットを受信」、「登録済み機器へパケットを送信」、「登録済み機器からのパケットを受信」、「未登録機器へパケットを送信」、「未登録機器からのパケットを受信」することを意味してい

る。これらのサービスを、登録済み機器もしくは未登録機器に対して、それぞれ許可するかどうかは図１１に示す別の設定ファイルに記述する。

【００３２】１００２は、このサービス一覧の書き方を定義するＤＴＤである。サービスには、属性値としてサービス名、３種類のサービス間の依存関係を定義している。AutoDependは、参照先のサービスに対して設定されている許可情報をそのまま受け継ぐことを意味する。PositiveDependは、参照先のサービスでの許可情報が「ＯＫ」であれば、この属性を付けたサービスでも自動的にＯＫになるという依存関係を意味する。NegativeDependは、逆に参照先のサービスの許可情報が「ＮＧ」であれば、この属性を付けたサービスでも自動的にＮＧになるという依存関係を意味する。この例では、ForwardFromInternetというサービスは、ReceiveFromRegisteredNodeというサービスに対してNegativeDepend属性を持っている。これは、「ＬＡＮ上の登録済み機器からのパケットの受信が禁止されているならば、インターネットからのパケットの受信も禁止とする」ことを意味する。

【００３３】図１１は、図１０で定義したサービスを、登録済み機器および未登録機器において許可するかどうかを設定した許可情報の例である。図１１において、１１０１は許可情報の例であり、１１０５はその記法を定義するＤＴＤである。１１０１では、機器ごとに図１０で定義したサービスに対する許可情報を定義する。１１０２は登録済み機器でのデフォルトの許可情報を定義している。１１０３は未登録機器でのデフォルトの許可情報を定義している。１１０４のように、個別の機器について許可情報を定義することもできる。

【００３４】図１３は、図１１に示した許可情報の内容を、図２と同様に表形式で表したものである。図２とは異なり、ここでは１１０４に示した個々の機器に関する許可情報が表の列１３０３として追加されている。このように表の列を追加することによって、デフォルトの設定以外にも機器ごとの特別な設定を、プログラムを変更することなく追加することができる。表の列を表す内容は、具体的には図１１の許可情報１１０１に対して、<node>エレメントを追記していくことで実現する。登録済み機器と未登録機器およびインターネット間とのパケットのやり取りを許可するかどうかは、それぞれの機器がパケットを受信した時に判定する。

【００３５】図１２に、図１０と図１１で示したサービス定義と許可情報を参照して、ＬＡＮ上でのパケットの送受信の制御を行う手順を示す。まず、パケットを受信した機器は自分のＭＡＣアドレスを元に機器プロパティ情報ＤＢ３０５を参照し、定義済みの機器名称を取得する（ステップ１２０１）。次に取得した機器名称を元に、図１１の許可情報ファイル１１０１を参照し、個別の許可情報が定義されているかどうか調べ、定義されていればそのnodeエレメントを読み込み、定義されていなければ名前が「RegNode-default」のnodeエレメントの内容を読み込む(ステップ１２０２)。

【００３６】次に、受信したパケットの送信元が同一ドメインかどうかを調べ（ステップ１２０３）、同一ドメイン内からのものであればそのパケットに含まれるＭＡＣアドレスから機器プロパティ情報ＤＢ３０５を検索する（ステップ１２０４）。そして、パケット送信元が登録済み機器かどうかを調べ（ステップ１２０５）、もし登録済み機器であれば、ステップ１２０２で読み込んだ許可情報の中のReceiveFromRegNodeがname属性の値になっているserviceエレメントを参照する（ステップ１２０６）。未登録であれば、同様にname属性の値がReceiveFromUnknowNodeであるserviceエレメントを参照する（ステップ１２０７）。また、ステップ１２０３でパケット送信元が同一ドメインでなければ、name属性の値がForwardFromInternetであるserviceエレメントを参照する（ステップ１２０８）。そして、参照したエレメントの値を調べ（ステップ１２０９）、「ＯＫ」であれば受信したパケットを処理する（ステップ１２１０）。「ＮＧ」であった場合はパケットを破棄する。

【００３７】以上のような手順を踏むことによって、重要度によってレベル分けした機器間でのパケットのやり取りを制御することが可能となり、不正に接続された機器がＬＡＮ１０２上に登録されている機器へ不正にアクセスすることを防ぐことができる。なお、インターネットとのパケットのやり取り、またはＬＡＮ上の機器同士での通信を許可するかどうかを設定する際に、機器の識別子ではなく機器の種別を指定することで同一種別の複数の機器に対して、機器ごとの個別の設定を省略するように構成することができる。このように構成した場合には、管理者の作業をさらに低減することが可能になる。

【００３８】

【発明の効果】以上説明した通り、本発明によれば、プラグアンドプレイの利便性を活かしつつ不正に接続された機器による被害を抑え、また、ネットワーク管理作業に関する高度な知識を必要とせずに、機器の重要度レベルに応じたアクセス制御および機器管理を実現することができる。

【図面の簡単な説明】

【図１】本発明を適用したネットワーク機器管理装置のネットワーク環境の例を示す図である。

【図２】登録済み機器と未登録機器に対するサービスの設定例を示す図である。

【図３】図１におけるネットワーク機器管理装置の内部構成を表すブロック図である。

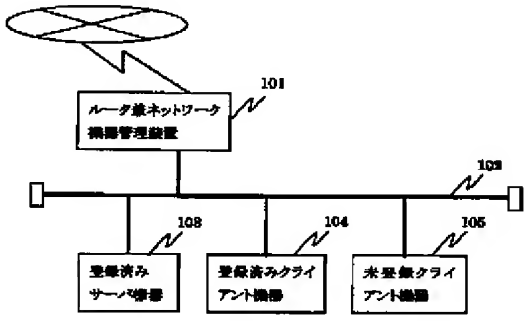
【図４】機器のプロパティ情報の例を示す図である。

【図５】図１におけるネットワーク機器管理装置の外観と画面表示例を示す図である。

【図６】ＬＡＮに接続されている機器の一覧を表示する処理のフローチャートである。

【図７】未登録機器を正当な機器として登録する処理のフローチャートである。
【図８】共通の機器プロパティ情報を提供する分散ＤＢが持つテーブルの例を示す図である。
【図９】分散ＤＢに対してＭＡＣアドレスから機器の種別情報を取得する処理のフローチャートである。
【図１０】ＬＡＮ上で利用可能なサービスの定義例である。
【図１１】ＬＡＮ上のサービスに対するアクセス許可情報の定義例である。
【図１２】ＬＡＮ上の機器に対するアクセスを許可するかどうかを判定する処理のフローチャートである。
【図１３】登録済み機器と未登録機器の他に個々の機器に対するサービスの設定例を示す図である。
【符号の説明】
１０１　ネットワーク機器管理装置
＊１０２　ＬＡＮ
１０３　登録済みサーバ機器
１０４　登録済みクライアント機器
１０５　未登録クライアント機器
３０１　ネットワーク接続／通信手段
３０２　ルーティング制御手段
３０３　機器プロパティ情報管理手段
３０４　機器プロパティ情報解析手段
３０５　機器プロパティ情報ＤＢ
３０６　アクセス制御適用手段
３０７　機器プロパティ情報表示手段
３０８　接続機器認識手段
４０１　機器プロパティ情報のＸＭＬインスタンス
５０２　機器一覧表示画面
１００１　サービス一覧を記述したＸＭＬインスタンス
＊　１１０１　アクセス許可情報

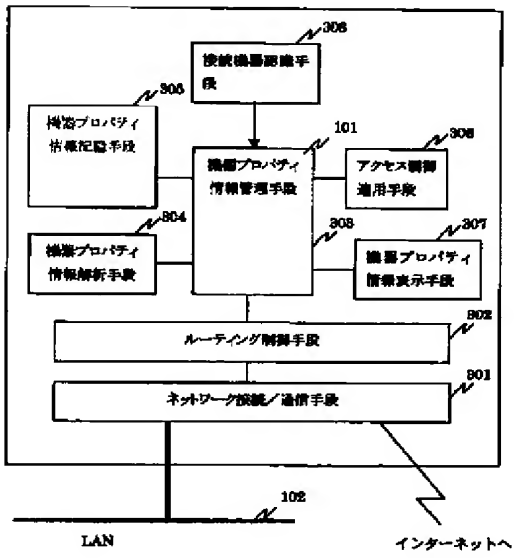
【図１】



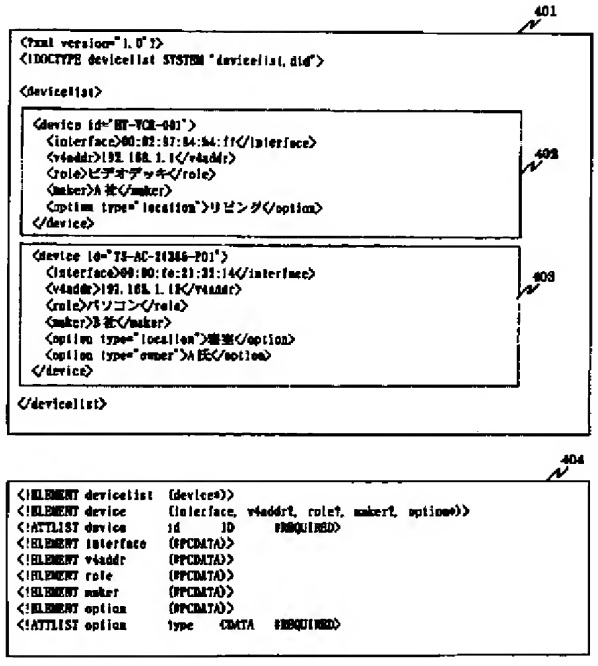
【図２】

	201 登録済み機器デフォルト	202 未登録機器デフォルト
インターネットへのパケット送信	○	×
インターネットからのパケット受信	○	×
登録済み機器へのパケット送信	○	○
登録済み機器からのパケット受信	○	×
未登録機器へのパケット送信	×	○
未登録機器からのパケット受信	○	○

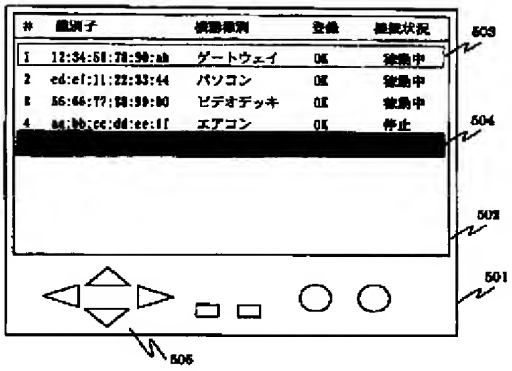
【図３】



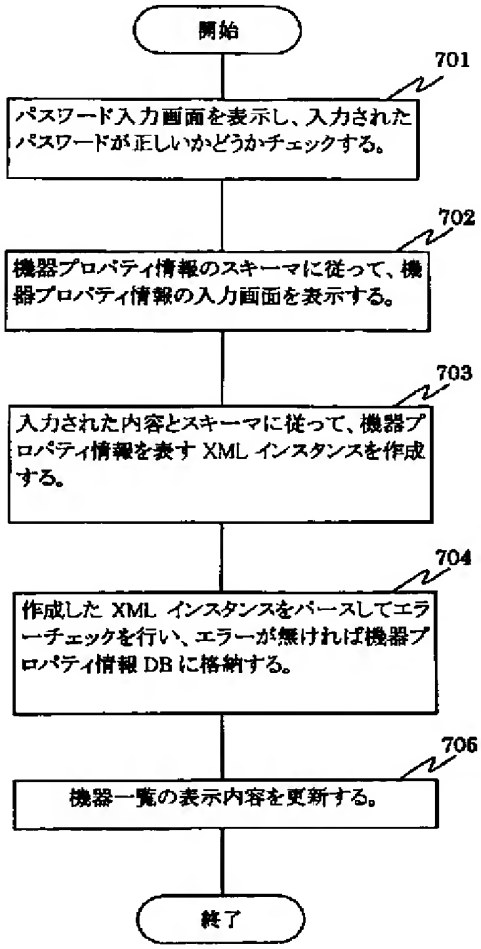
【図４】



【図５】



【図７】



【図８】

(a)

801

メーカ識別子	問合せ先 IP アドレス
aabbcc	255:1000:555:777:128
012345	2001:1201:765:111:33:44:55
112233	2001:3200:999:bbb::3
...	...

(b)

802

製品識別子	機器情報格納先
ddeeff	"product0001.xml"
6789ab	"product0002.xml"
...	...

【図１０】

1001

```
<?xml version="1.0" encoding="Shift_JIS"?>
<!DOCTYPE services SYSTEM "services.dtd">

<services version="20010402">
  <service id="ForwardToInternet" />
  <service id="ForwardFromInternet"
           NegativeDepend="ReceiveFromRegNode" />
  <service id="SendToRegNode" />
  <service id="ReceiveFromRegNode" />
  <service id="SendToUnknownNode" />
  <service id="ReceiveFromUnknownNode" />
</services>
```

1002

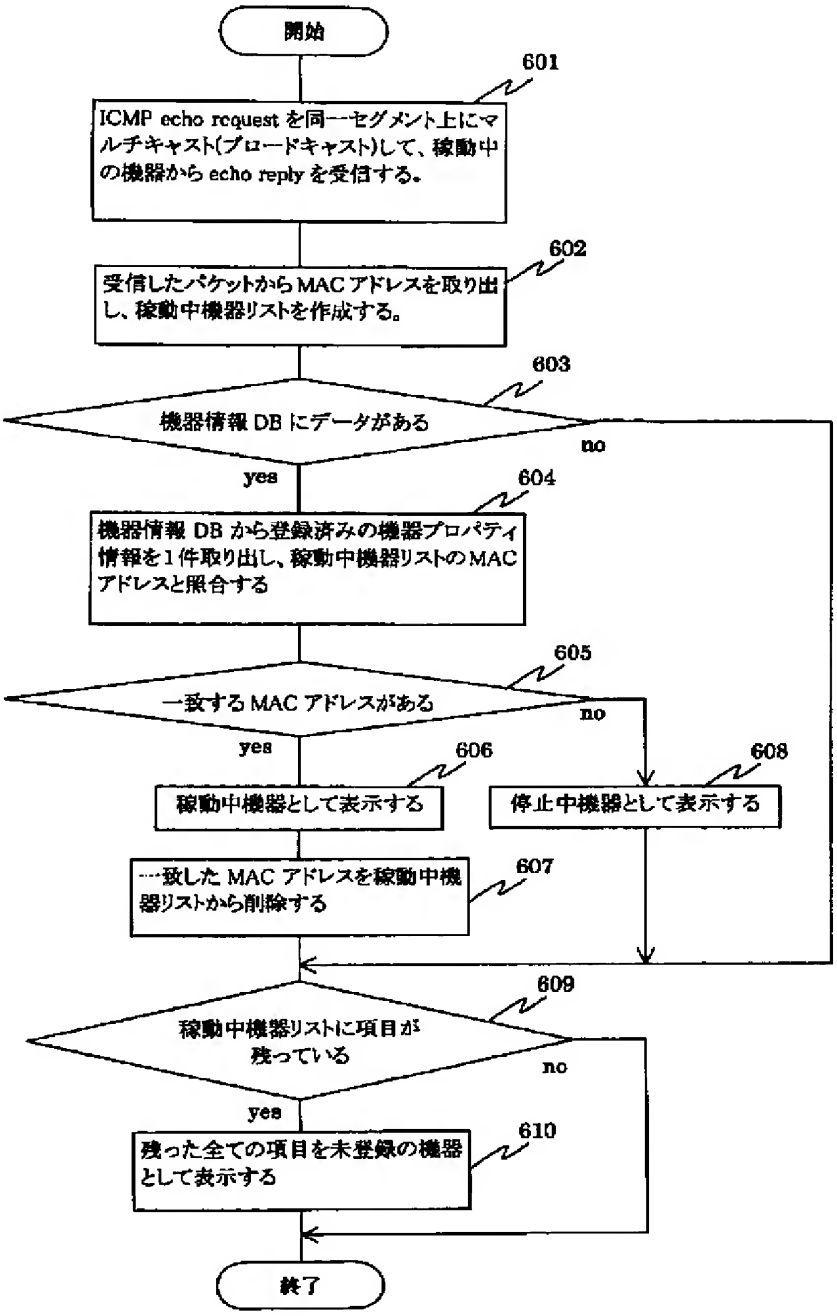
```
<!ELEMENT services (service)>
<!ATTLIST services version #ATTRIBUTE #REQUIRED>

<!ELEMENT service  (#PCDATA)>
<!ATTLIST service  id              ID     #REQUIRED
                   RuleDepend     IDREF  #IMPLIED
                   PositiveDepend IDREF  #IMPLIED
                   NegativeDepend IDREF  #IMPLIED
>
```

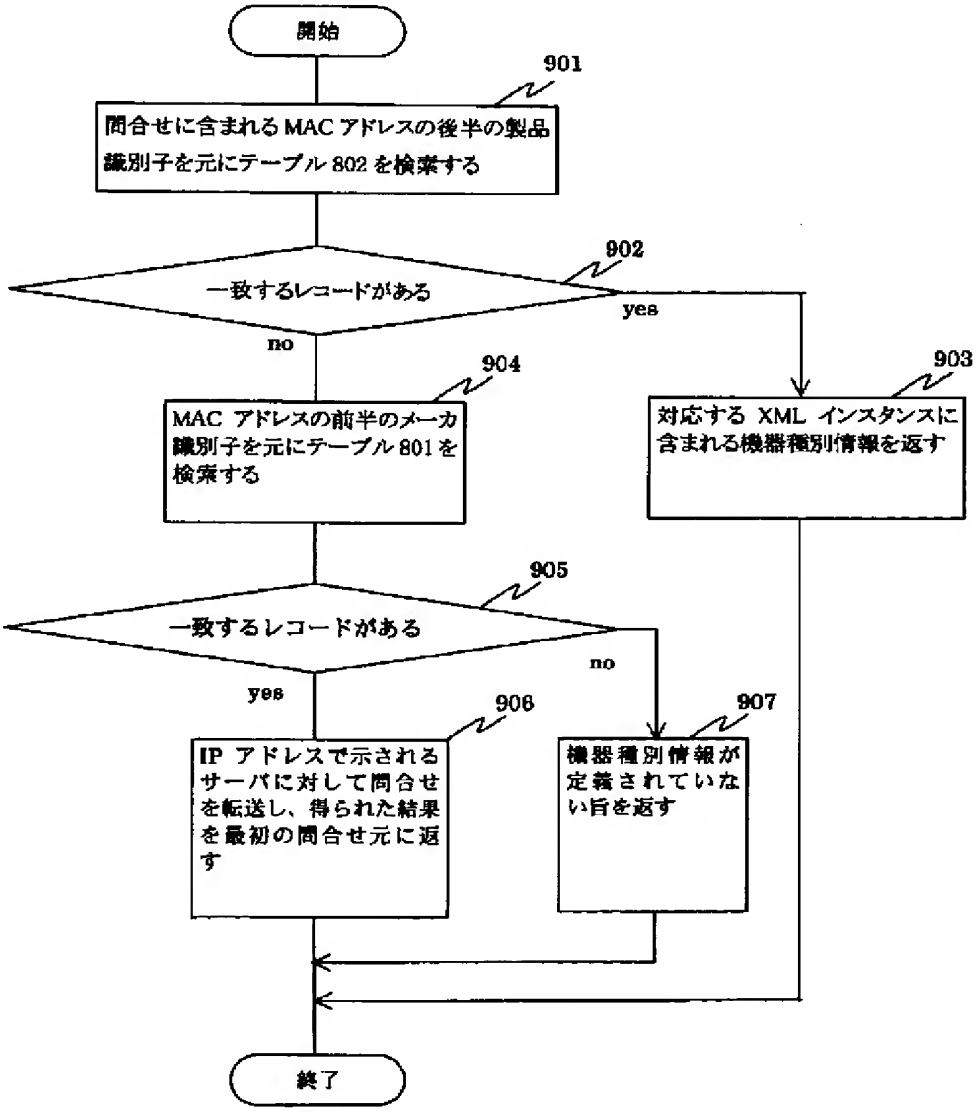
【図１３】

	1301 登録済み機器 デフォルト	1302 未登録機器 デフォルト	1303 HT-VCH-001 専用の設定
インターネットへのパケット送信	○	×	○
インターネットからのパケット受信	○	×	×
登録済み機器へのパケット送信	○	○	○
登録済み機器からのパケット受信	○	×	○
未登録機器へのパケット送出	×	○	○
未登録機器からのパケット受信	○	○	○

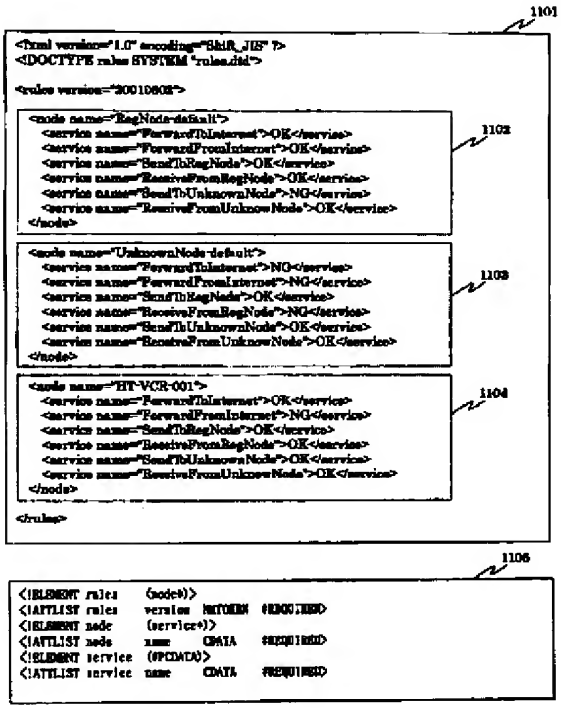
【図６】


開始
601
ICMP echo request を同一セグメント上にマルチキャスト(ブロードキャスト)して、稼動中の機器から echo reply を受信する。
602
受信したパケットから MAC アドレスを取り出し、稼動中機器リストを作成する。
603
機器情報 DB にデータがある
no
yes
604
機器情報 DB から登録済みの機器プロパティ情報を１件取り出し、稼動中機器リストの MAC アドレスと照合する
605
一致する MAC アドレスがある
no
yes
606
稼動中機器として表示する
608
停止中機器として表示する
607
一致した MAC アドレスを稼動中機器リストから削除する
609
稼動中機器リストに項目が残っている
no
yes
610
残った全ての項目を未登録の機器として表示する
終了

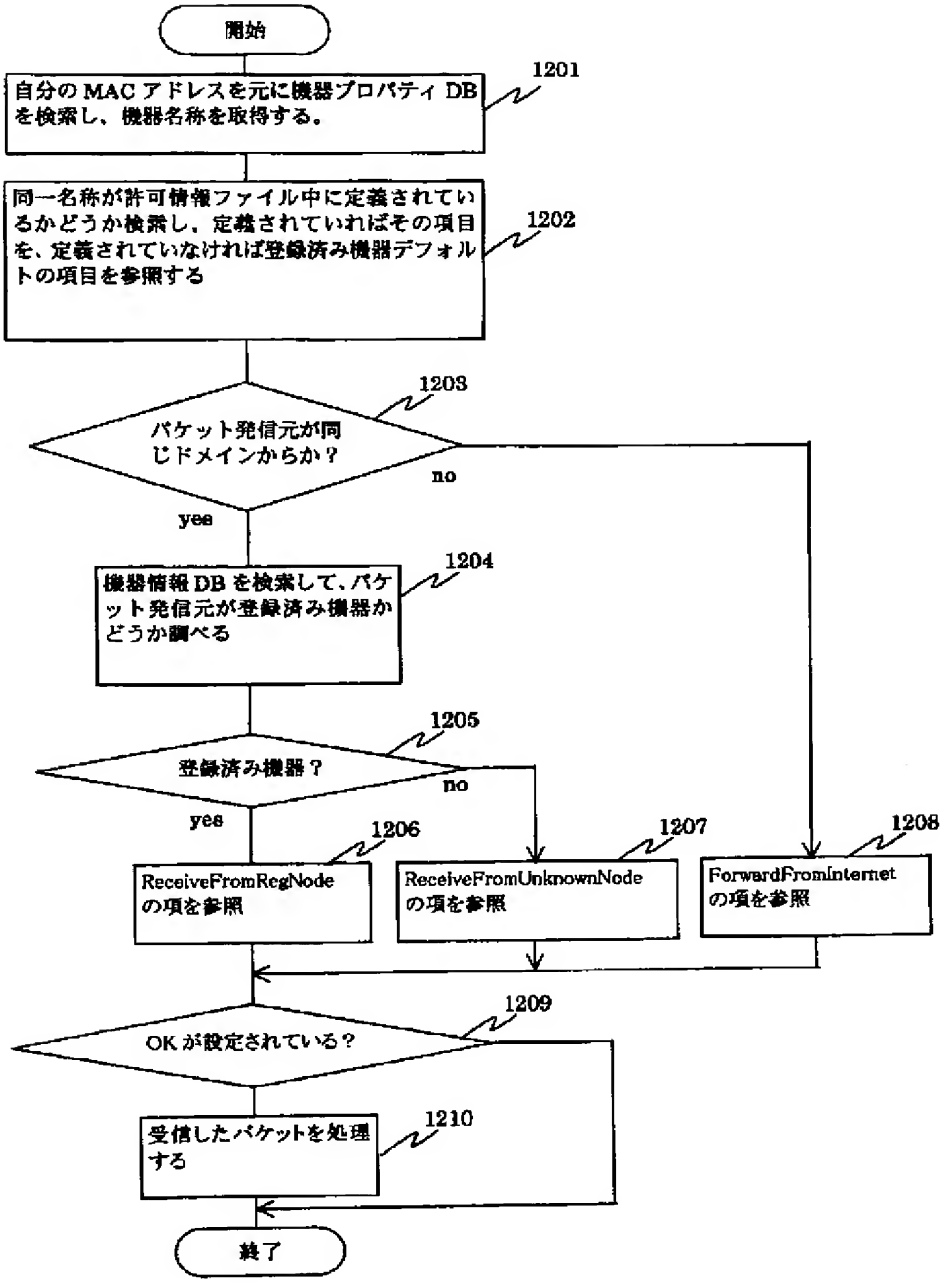
【図９】


開始
901
問合せに含まれるMACアドレスの後半の製品識別子を元にテーブル802を検索する
902
一致するレコードがある
yes
no
903
対応するXMLインスタンスに含まれる機器種別情報を返す
904
MACアドレスの前半のメーカ識別子を元にテーブル801を検索する
905
一致するレコードがある
yes
no
906
IPアドレスで示されるサーバに対して問合せを転送し、得られた結果を最初の問合せ元に返す
907
機器種別情報が定義されていない旨を返す
終了

【図１１】


1101
<?xml version="1.0" encoding="Shift_JIS" ?>
<!DOCTYPE rules SYSTEM "rules.dtd">
<rules version="20010803">
<node name="RegNode-default">
<service name="ForwardToInternet">OK</service>
<service name="ForwardFromInternet">OK</service>
<service name="SendToRegNode">OK</service>
<service name="ReceiveFromRegNode">OK</service>
<service name="SendToUnknownNode">NG</service>
<service name="ReceiveFromUnknowNode">OK</service>
</node>
1102
<node name="UnknownNode-default">
<service name="ForwardToInternet">NG</service>
<service name="ForwardFromInternet">NG</service>
<service name="SendToRegNode">OK</service>
<service name="ReceiveFromRegNode">NG</service>
<service name="SendToUnknownNode">OK</service>
<service name="ReceiveFromUnknowNode">OK</service>
</node>
1103
<node name="HT-VCR-001">
<service name="ForwardToInternet">OK</service>
<service name="ForwardFromInternet">NG</service>
<service name="SendToRegNode">OK</service>
<service name="ReceiveFromRegNode">OK</service>
<service name="SendToUnknownNode">OK</service>
<service name="ReceiveFromUnknowNode">OK</service>
</node>
1104
</rules>
1105
<!ELEMENT rules (node*)>
<!ATTLIST rules version NMTOKEN #REQUIRED>
<!ELEMENT node (service*)>
<!ATTLIST node name CDATA #REQUIRED>
<!ELEMENT service (#PCDATA)>
<!ATTLIST service name CDATA #REQUIRED>

【図１２】


開始
自分のMACアドレスを元に機器プロパティDBを検索し、機器名称を取得する。
1201
同一名称が許可情報ファイル中に定義されているかどうか検索し、定義されていればその項目を、定義されていなければ登録済み機器デフォルトの項目を参照する
1202
パケット発信元が同じドメインからか？
1203
no
yes
機器情報DBを検索して、パケット発信元が登録済み機器かどうか調べる
1204
登録済み機器？
1205
no
yes
ReceiveFromRegNodeの項を参照
1206
ReceiveFromUnknownNodeの項を参照
1207
ForwardFromInternetの項を参照
1208
OKが設定されている？
1209
受信したパケットを処理する
1210
終了